IN THE CLAIMS:

The current claims follow. For claims not marked as amended in this response, any difference in the claims below and the previous state of the claims is unintentional and in the nature of a typographical error.

1. (Currently Amended) A router for interconnecting external devices coupled to said router, said router comprising:

a switch fabric; and

a plurality of routing nodes coupled to said switch fabric, wherein each of said plurality of routing nodes:

a first network processor comprising a first plurality of microengines, each of said first plurality of microengines for performing first security and classification functions associated with data packets received from said external devices and transmitted to said switch fabric, wherein each data packet is distributed to a selected microengine; ~~and~~

a second network processor comprising a second plurality of microengines, each of said second plurality of microengines for performing second security and classification functions associated with data packets received from said switch fabric and transmitted to said external devices, wherein each data packet is distributed to a selected microengine; and

a routing table search circuit comprising an initial content addressable memory stage followed by a plurality of trie tree search table stages.

2. (Previously Presented) The router as set forth in Claim 1 wherein said first and second security and classification functions comprise replacing a source address associated with header information of a first data packet with an address selected from a pool of router addresses associated with said router.

3. (Previously Presented) The router as set forth in Claim 1 wherein said first and second security and classification functions comprise filtering a first data packet based on at least one of: 1) a Layer 2 address associated with said first data packet; 2) a Layer 3 address associated with said first data packet; and 3) a traffic type associated with said first data packet.

4. (Previously Presented) The router as set forth in Claim 1 wherein said first and second security and classification functions comprise filtering a first data packet based on at least one of: 1) a Layer 4 address associated with said first data packet; and 2) a class of service (CoS) value associated with said first data packet.

5. (Previously Presented) The router as set forth in Claim 1 wherein said first and second security and classification functions comprise performing a Network Address Translation (NAT) function to provide subnet independence.

6. (Original) The router as set forth in Claim 1 wherein a first one of said first plurality of microengines is capable of executing N threads, wherein each of said N threads performs at least one security and classification function.

7. (Original) The router as set forth in Claim 6 wherein a first one of said second plurality of microengines is capable of executing M threads, wherein each of said M threads performs at least one security and classification function.

8. (Cancelled).

9. (Cancelled).

10. (Currently Amended) A communication network comprising a plurality of routers that communicate data packets to one another and to interfacing external devices, each of said plurality of routers comprising:

a switch fabric; and

a plurality of routing nodes coupled to said switch fabric, wherein each of said plurality of routing nodes:

a first network processor comprising a first plurality of microengines, each of said first plurality of microengines for performing first security and classification functions

associated with data packets received from said external devices and transmitted to said switch fabric, wherein each data packet is distributed to a selected microengine; ~~and~~

a second network processor comprising a second plurality of microengines, each of said second plurality of microengines for performing second security and classification functions associated with data packets received from said switch fabric and transmitted to said external devices, wherein each data packet is distributed to a selected microengine; and

a routing table search circuit comprising an initial content addressable memory stage followed by a plurality of trie tree search table stages.

11. (Previously Presented) The communication network as set forth in Claim 10 wherein said first and second security and classification functions comprise replacing a source address associated with header information of a first data packet with an address selected from a pool of router addresses associated with said router.

12. (Previously Presented) The communication network as set forth in Claim 10 wherein said first and second security and classification functions comprise filtering a first data packet based on at least one of: 1) a Layer 2 address associated with said first data packet; 2) a Layer 3 address associated with said first data packet; and 3) a traffic type associated with said first data packet.

13. (Previously Presented) The communication network as set forth in Claim 10 wherein said first and second security and classification functions comprise filtering a first data packet based on at least one of: 1) a Layer 4 address associated with said first data packet; and 2) a class of service (CoS) value associated with said first data packet.

14. (Previously Presented) The communication network as set forth in Claim 10 wherein said first and second security and classification functions comprise performing a Network Address Translation (NAT) function to provide subnet independence.

15. (Original) The communication network as set forth in Claim 10 wherein a first one of said first plurality of microengines is capable of executing N threads, wherein each of said N threads performs at least one security and classification function.

16. (Original) The communication network as set forth in Claim 15 wherein a first one of said second plurality of microengines is capable of executing M threads, wherein each of said M threads performs at least one security and classification function.

17. (Cancelled).

18. (Cancelled).

19. (Currently Amended) For use in a router comprising a switch fabric and a plurality of routing nodes coupled to the switch fabric, each of the routing nodes for transmitting data packets to, and receiving data packets from, external devices and transmitting data packets to, and receiving data packets from, other routing nodes via the switch fabric, a method ~~of performing security and classification functions~~ comprising the steps of:

performing routing table searching using an initial content addressable memory stage followed by a plurality of trie tree search table stages;

performing first security and classification functions in a first network processor comprising a first plurality of microengines, each of said first plurality of microengines capable of executing said first security and classification functions, wherein the first network processor processes data packets being transmitted from the external devices to the switch fabric, and wherein each data packet is distributed to a selected microengine; and

performing second security and classification functions in a second network processor comprising a second plurality of microengines, each of the second plurality of microengines capable of executing the second security and classification functions, wherein the second network processor processes data packets being transmitted from the switch fabric to the external devices, and wherein each data packet is distributed to a selected microengine.

20. (Previously Presented) The method as set forth in Claim 19 wherein the first and second security and classification functions comprise replacing a source address associated with header information of a first data packet with an address selected from a pool of router addresses associated with the router.

21. (Previously Presented) The method as set forth in Claim 19 wherein the first and second security and classification functions comprise filtering a first data packet based on at least one of: 1) a Layer 2 address associated with the first data packet; 2) a Layer 3 address associated with the first data packet; and 3) a traffic type associated with the first data packet.

22. (Previously Presented) The method as set forth in Claim 19 wherein the first and second security and classification functions comprise filtering a first data packet based on at least one of: 1) a Layer 4 address associated with the first data packet; and 2) a class of service (CoS) value associated with the first data packet.

23. (Previously Presented) The method as set forth in Claim 19 wherein the first and second security and classification functions comprise performing a Network Address Translation (NAT) function to provide subnet independence.